ppes

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,963	01/10/2001	John S. Flowers	HVWD-01008US0 MEM/SBS	9385

758 7590 05/27/2003

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	13

DATE MAILED: 05/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/757,963	Applicant(s) FLOWERS ET AL.
	Examiner Aravind K Moorthy	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4, 9* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 5-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 5-28 are directed to software for gathering information about the network to determine vulnerabilities of a host on the network and for examining network traffic responsive to the vulnerabilities determined by the vulnerability detection system to detect traffic indicative of malicious activity. Page 26 of the specification discloses that the VDS and IDS could be implemented as software. A program is in and of itself non-statutory subject matter that does not fall within the realm of 35 USC 101. Actually a program is more akin to non-functional data, as software cannot without aid of a device such as a computer perform any of the recited functions. Software not embodied on a computer readable medium is non-statutory, as they do not fall within any of the statutory classes listed in 35 U.S.C 101.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 14, 26 and 38 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter that was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

This is an invention for a vulnerability detection system (VDS) and an intrusion detection system (IDS). As understood by the examiner, the invention is directed to vulnerability detection systems, intrusion detection systems, communication between the two, and query-based rules for identifying vulnerabilities and detecting intrusions. Applicant fails to mention how to verify the determined vulnerabilities, page 7. The examiner asserts that one of ordinary skill would have to go through undue experimentation to find the theory behind the invention. The applicant does not discuss how the vulnerabilities are verified and how the IDS is adapted to detect traffic indicative of exploitations of only the verified vulnerabilities. Without such details, one skilled in the art would be required to engage in undo experimentation in order to practice or use the invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 40 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 40 recites the limitation "the updating" in the claim. There is insufficient antecedent basis for this limitation in the claim. There is no limitation of "the updating" in claim 29. For the sake of examining, the examiner assumes that claim 40 is dependent on claim 39.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 5-14, 17-26 and 29-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Gleichauf et al U.S. Patent No. 6,415,321 B1 in view of Microsoft Computer Dictionary (hereinafter Microsoft).

As to claims 5, 13, 17, 25, 29 and 37, Gleichauf discloses a vulnerability detection system (VDS) [acquisition engine **48**] for gathering information about the network **12** to determine vulnerabilities of devices coupled to a network [column 4 lines 1-21]. Gleichauf discloses that two of the devices couple to the network is web server **30**, terminal sever **28** and file server **34**. Gleichauf discloses an intrusion detection system [IDS] for examining network traffic responsive to the vulnerabilities determined by the VDS to detect indicative of malicious activity [column 4 lines 37-39].

Microsoft defines a **host** as server computer that has access to other computers on the network, page 256.

Network devices **30**, **28** and **34** are all servers that have access to workstations **32**, **36**, **38** and **40**. Based on the definition from Microsoft, the examiner asserts that network devices **30**, **28** and **34** are hosts.

As to claims 6, 18 and 30, Gleichauf discloses that the VDS is adapted to gather information about the network by sending data to the host and receiving responsive data from the host [column 4 lines 3-6]. Gleichauf discloses network information is gathered by pinging devices coupled to the network [i.e. web server **30**, terminal sever **28** and file server **34**].

Microsoft defines pinging as a protocol for testing whether a particular computer is connected to the Internet by sending a packet to its IP address and waiting for a response.

Based on the definition from Microsoft, the examiner asserts that data is sent [i.e. packets] and responsive data [i.e. network data] is received from the host.

As to claims 7, 19 and 31, Gleichauf discloses that the VDS is adapted to gather information automatically provided by the host. Based on the definition of pinging, discussed above, data is going to be automatically sent by the host to the VDS by pinging the network.

As to claims 8, 20, and 32, Gleichauf discloses a vulnerabilities rules database [hypercube storage **50**], which is in communication with the VDS [figure 3], for storing rules describing vulnerabilities of the host [column 6 lines 31-46]. Gleichauf discloses that the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the host [column 7 lines 25-45].

As to claim 9, Gleichauf discloses that the VDS is adapted to analyze the gathered information with the rules to identify an operating system on the host and determine the vulnerabilities responsive to the operating system [abstract].

As to claim 10, Gleichauf discloses that the VDS is adapted to analyze the gathered information with the rules to identify an open port on the host and determine the vulnerabilities based on the open port [column 4, lines 3-6; column 5, lines 15-31].

As to claims 11, 23 and 35, the examiner asserts that the rejection as discussed above for an operating system applies to an application.

Microsoft defines an application as a program designed to assist in the performance of a specific task. Microsoft defines an operating system as the software that controls the allocation and usage of hardware resources such as memory, central processing unit (CPU) time, disk space, and peripheral devices, page 378. The examiner asserts that controlling the allocation and usage of hardware resources are both specific tasks. Thus, the examiner asserts that an operating system is an application. The rejection applied to claim 9 above is also applied to claims 11, 23 and 35.

As to claims 12, 24 and 36, Gleichauf discloses an intrusion rules database, in communication with the IDS, for storing rules describing malicious activity and that the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities [column 7, lines 31-53 of U.S. Patent No. 6,324,656 incorporated by reference].

As to claims 14, 26 and 38, Gleichauf discloses that the VDS is adapted to verify the determined vulnerabilities and the IDS is adapted to detect traffic indicative of exploitations of

only the verified vulnerabilities [column 4, lines 52-55 of U.S. Patent No. 6,324,656 incorporated by reference].

As to claims 21 and 33, Gleichauf discloses determining vulnerabilities comprises analyzing the gathered information with the rules to identify an operating system on the host [column 5 lines 15-30].

As to claims 22 and 34, Gleichauf discloses determining vulnerabilities comprises analyzing the gathered information to identify an open port on the host [column 5, lines 15-31].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 15, 16, 27, 28, 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al U.S. Patent No. 6,415,321 B1 and Microsoft Computer Dictionary (hereinafter Microsoft) as applied to claims 5 and 17 above, and further in view of examiner's official notice.

As to claims 15, 16, 27 and 28, the Gleichauf-Microsoft combination does not teach that the VDS is adapted to update the determined vulnerabilities and that the IDS is adapted to detect traffic indicative of malicious activity in response to the update. The Gleichauf-Microsoft combination does not teach that the VDS is adapted to update the determined vulnerabilities in response to a change in the network.

The examiner takes official notice that new network devices are added to a network and that new network devices introduce new vulnerabilities.

The Gleichauf-Microsoft combination would have included that the new vulnerabilities would have been updated and that the IDS would have detected traffic indicative of malicious traffic with respect to the updated vulnerabilities. New vulnerabilities would have been detected if new devices are introduced on the network and the IDS would have detected traffic indicative of malicious traffic with respect to the updated vulnerabilities.

The motivation to modify the Gleichauf-Microsoft combination would have been to protect the network from new exploitations and malicious traffic when new network devices and vulnerabilities are introduced.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O Hayes can be reached on 703-305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

May 14, 2003

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100